Open Trusted Technology Forum Overview (OTTF)

v1.5

"Build with Integrity

Buy with Confidence "

Note: OTTF Materials are copyrights of The Open Group
All information presented is subject to change

THE Open GROUP
Making standards work®

The Technology Supply Chain Integrity Challenge

- Perceived increase in sophistication and severity of cybersecurity attacks worldwide
- Potential for vulnerabilities introduced by use of technology provided through the global supply chain
- Governments and organizations buy products from companies they trust, but those companies usually do not manufacture all the components of their products
- The forum is being formed in response to the need to establish industry best practices that will help understand and reduce risks posed by the globalization of the technology supply chain

THE Open GROUP
Making standards work®

The OTTF will respond to these industry challenges by…

- Reducing risks that may be introduced from global supply chain providers
- Identifying manufacturing practices and checkpoints throughout the lifecycle that mitigate risk from uncontrolled, unprotected development methods and engineering procedures
- Develop conformance and accreditation criteria for trusted technology providers that will instill trust and confidence in both providers and consumers
- Work with the global community to develop responsible and realistic procurement policies that mitigate the risks introduced from supply chain vulnerabilities for all governments and vertical industries

The Open Group

- The Open Group **works with customers, suppliers, consortia, and other standards bodies to**
  - Capture, understand, and address current and emerging requirements, and establish policies and share best practices
  - Facilitate interoperability, develop consensus, and evolve and integrate specifications and open source technologies
  - Offer a comprehensive set of services to enhance the operational efficiency of consortia
  - Operate the industry's premier certification service
- **Vision of Boundaryless Information Flow™** – with enterprise architecture as a critical element for making the vision a reality, the TOGAF Architecture Development Method (ADM) provides an important toolset
- **"Making Standards Work™"** – extensive experience and track record in facilitating consensus to develop standards and operating a premier certification service

The Open Group's Platinum Members

Capgemini
hp
IBM
Kingdee
ORACLE
SAP

THE Open GROUP
Making standards work™

Architecture Practitioner Conferences

Core Technology

LDAP / CCI

MILS

AQRM

Motif®

DRDA®

DCE

(Open DCE)

Forums

- ✓Architecture
- ✓Platform
- ✓ Jericho & Security
- ✓Identity Management
- ✓Enterprise Management
- ✓Real Time and Embedded Systems

Certifications

- UNIX
- LDAP
- WAP
- S/MIME
- ITAC / ITSC
- NASPL

Master Certified IT Architect

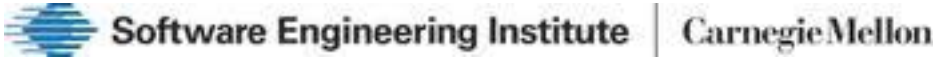
LDAP Certified

Methods & Best Practices

SOA-WG

THE Open GROUP
Making standards work®

Open Trusted Technology Forum Membership



As of February, 2011

Our Vision and Mission

OTTF Vision:

We are a global consortium established to support the adoption of best practices for secure technology engineering and procurement strategies in order to develop a more trustworthy global technology supply chain.

OTTF Mission:

The Trusted Technology Forum is an open, vendor-neutral initiative that formulates and supports use of a global framework, guidelines, procurement strategies and related resources that can

- Help the technology industry "*build with integrity*"
- Enable customers to "*buy with confidence"*; and
- Support global innovation.

THE Open GROUP
Making standards work®

What Problems Are We Solving?

- Commercial technology comprises key components of our critical infrastructure
- It's become necessary to understand;
  - The **potential integrity risks** that may be inherited from supply chains, both for software and hardware, and how the original equipment manufacturer (OEM) assesses and manages these risks;
  - Practices that can **mitigate potential risks** of significant supply chain attacks;
  - Risks to confidentiality, integrity, and availability of a customer's environment or critical infrastructure as a result of procurement by customers of **counterfeit components and products**;
  - Which software or technology **development or engineering practices** can help reduce product security and integrity risks;
  - How product assurance and risk is managed through the adoption of **industry best practices and recognized international and open industry standard**s.

THE Open GROUP
Making standards work®

Need to Work Together to Develop Expectations for a Trusted Commercial off the Shelf (COTS) IT Product

- "Good Commercial Product" – Helpful information that builds understanding of the product
  - What's in it (source code and origin/pedigree)
  - How was it built (development and manufacturing)
  - How will it be sustained from an OEM perspective
  - What management, process and quality controls were applied
  - What are the meaningful supply chain considerations
  - What variability, and volatility of sub-processes and supply should be expected (opportunistic component sourcing and contract fabrication)
  - What other "measures of goodness" can be used or leveraged
  - Not a substitute for CC, NIST, or ITU; Interoperability or protocol level compliance or certification

What are the Realistic, Consumable, Affordable Industry Best Practices?

THE Open GROUP
Making standards work®

TTF Industry Driven Consensus Approach

- Identify and gain consensus on common processes, techniques, methods, product and system testing procedures, and language to describe and guide product development and supply chain management practices:
  - **Identify product assurance practices** that should be expected from all commercial technology suppliers based on expected risks and the baseline best practices of leading trusted commercial technology suppliers
  - Help **establish expectations for global government and commercial customers** when seeking to identify a trusted technology supplier
  - **Leverage existing** globally recognized information assurance practices and **standards – Not an alternative to CC, NIST**
  - Share with commercial technology consumers secure development and manufacturing and **trustworthy technology supplier best practices**
  - **Harmonize global standards & language** used to describe best practices

Value of an Industry Lead Approach

- Need to understand: What is a “Good Commercial Product”
  - **Multiple efforts** (many still ongoing) by governments to prescribe standards for strength of IT security products, e.g. Crypto, Common Criteria, IPv6, etc. This assumes that products are designed and developed to meet established criteria. What if the goal is to simply acquire “good commercial products?” How does the technology industry identify a “good or trusted commercial product”
  - **Customers seek** lower cost/higher performance commercial building blocks for secure IT systems
  - **Industry can benefit immensely:**
    - Qualitative brand differentiation
    - Leverage existing corporate best practices that comply
    - Opportunity to define and dispel globalization concerns

“Build with Integrity Buy with Confidence”™

THE Open GROUP
Making standards work®

TTF Standards Development Principles

Principles for accomplishing our mission:

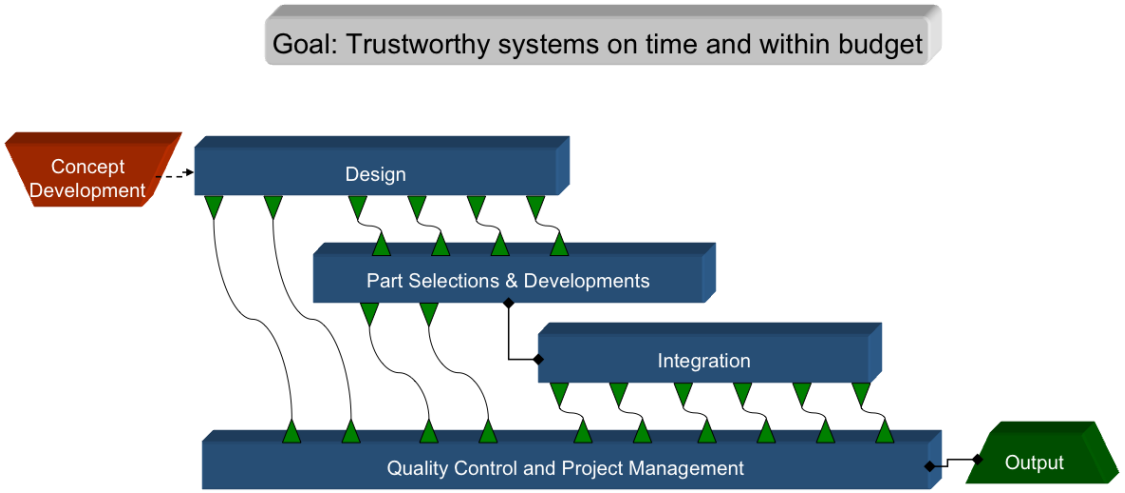
Our mission will be accomplished by providing vendors, distributors, integrators and consumers commercially reasonable integrity practices that are;

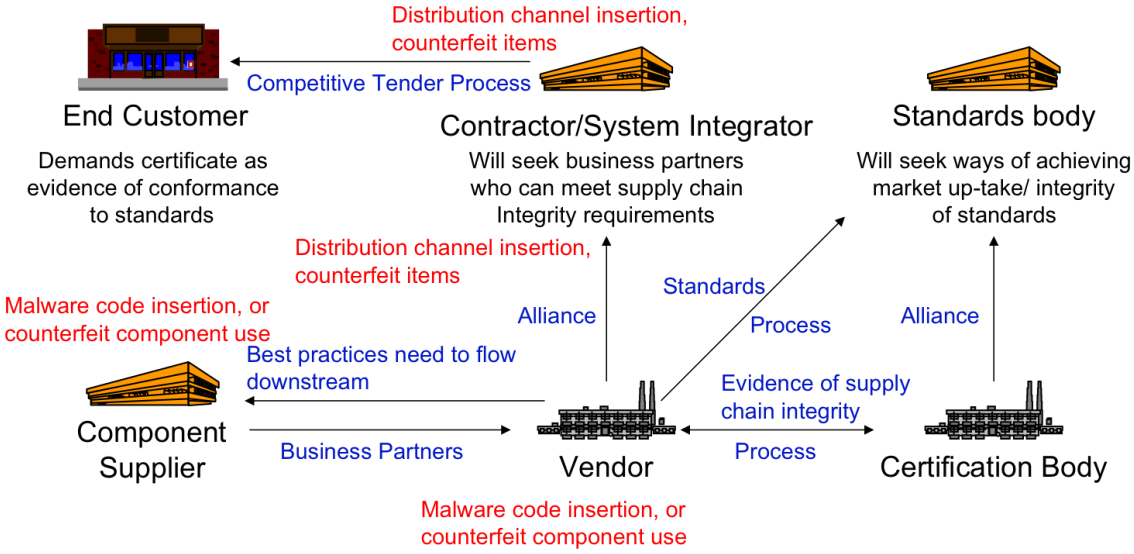
- Realistic - Based on a real, evidence based understanding of the risk
- Practical and effective – Practitioner based, evidence that it works in the field
- Reasonable – Achievable and implementable by a wide variety of vendors and stakeholders
- Affordable – Reasonably cost effective to implement
- Open – Based on open standards and recognized industry best practices

THE Open GROUP
Making standards work®

ACS Initiative Work Products

- Developed Business Scenario White Paper
- Defined Ecosystem
- Customer Pain Points
- Problem to be solved
- Created Initial TTPF
- Operational Vision





➢ Mitigate vulnerabilities which could lead to exploitation and malicious threats to product integrity.

THE Open GROUP
Making standards work®

Trusted Technology Provider Definitions

- **Supply Chain Attack (general)**
  In general, a supply chain attack is an attempt to disrupt the creation of goods by subverting a commercial manufacturing, ordering, or distribution process.
- **Supply Chain Integrity**
  The manufacturing and/or development process performs its intended function in an unimpaired manner, free from deliberate or inadvertent manipulation. Extends NIST definition [NIST 800-12].[1]
- **Technology Supply Chain Attack**
  A technology supply chain attack subverts the hardware, software, or configuration of a product, prior to customer delivery, for the purpose of introducing an exploitable vulnerability.
- **Technology Supply Chain**
  The manufacturing and/or development process used to produce and deliver hardware or software technology products and their configuration.

[1] NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook; refer to: http://csrc.nist.gov/publications/PubsSPs.html.

THE Open GROUP
Making standards work®

Trusted Technology Provider Framework

- Grouping of industry best practices by category.
- Best practices of most mature industry technology vendors
- For example, a supplier implements a Secure Engineering/Development Method.
- Simple but not simplistic
- Realistic, consumable, actionable, affordable for technology vendors in a global environment

THE Open GROUP
Making standards work®

Open Trusted Technology Provider Framework (O-TTPF)

The framework is broken into categories of Industry Best Practices:

- Product Development /Engineering
- Secure Development / Engineering
- Supply Chain Integrity
- Product Evaluation Practices

THE Open GROUP
Making standards work®

O-TTPF Best Practice Categories

Best Practice Categories	Definition
Product Engineering / Development Method	Trusted technology providers utilize and internalize the application of a well-formed and documented development (or manufacturing) method or process.
Secure Engineering / Development Method	Secure development methods include techniques such as secure code design reviews or threat modeling, risk assessment and tooling for detecting, fixing, and mitigating vulnerabilities in both software and hardware. They might also include run-time protection measures; or monitoring and corrective actions for third-party component vulnerabilities or risks. Product design may also employ ways to ensure authenticity and protection from counterfeit components and use run-time execution protection measures; for example, the use of code signing.
Supply Chain Management Method	Trusted technology providers manage their supply chains through the application of defined, monitored, and validated supply chain processes. These practices seek to ensure the integrity of the supply chain throughout product design, sourcing, fabrication delivery, support, and end-of-life.
Product Evaluation Methods	A Trusted Supplier submits Information Assurance (IA) and IA-enabled products to one or more mutually recognized standards-based evaluation processes to determine the fulfilment of particular security properties, to levels of assurance appropriate to the application of the product depending on the needs of the market. (Common Criteria is an example of one such process).

Example O-TTPF Best Practice and Guidance

Industry Best Practice	Guidance
Trusted technology providers utilize and internalize the application of a well-formed and documented development (or manufacturing) method or process.	Engineering/development methods are practical and meaningful within the vendor's domain of software, firmware, or hardware manufacturing. This can be measured in the following ways: 1. The method must be demonstrably successful in practice. Successful means two things: • When used correctly, the method routinely has the effects it claims to provide. • The results routinely satisfy the needs of the method's constituencies. 2. The method is maintained by an active community of practitioners. 3. The method must have explicitly defined inputs, participants, roles, process steps, outputs, results, and deliverables. 4. The method must be supported by self-paced or instructor-led training to a published, common curriculum. 5. The method must be supported by collateral materials for use by practitioners. These materials might include, for example, templates, tools, examples, and best practice recommendations. 6. The method must have a defined process for feedback from practitioners and the maintenance and revision of the above materials (community, documentation, training, and collateral). 7. The method supports the defined attributes of a well formed engineering/development method as defined in "Best Practice Attributes"

Sample O-TTPF Conformance Requirements

Category: Product Engineering / Development

O-TTPF Mapping	Conformance Statement	Evidence Requirements
Product Engineering/ Development Method	Trusted technology providers utilize and internalize the application of a well-formed and documented development (or manufacturing) method or process.	Applicant must provide evidence of the use of a meaningful method as defined by the method recognition criteria. {As defined by TTPF Method Guidance}
Product Engineering / Development Method	Product engineering methods are specified and refined to best fit the engineering / development characteristics of the target product.	Applicant must explain: a. How the method meets the needs of the engineering/ development team. b. How the method has been refined to meet the characteristics of the target product.
Product Engineering / Development Method Requirements Management	Product requirements are documented and traced back to implemented product functionality. Product functionality are traced back to functional requirements.	Applicant provides example of documented product requirements and traceability matrix (or equivalent).
Product Engineering / Development Method Formal Product Engineering or Development Community	Product lifecycle practices and processes are supported by a community of practitioners who vigilantly maintain the organization's engineering practices.	Applicant provides evidence that engineering / development practices are maintained, evolve and grow through the feedback and contributions of a community of practitioners.

NOTE: For use as Example Only

THE Open GROUP
Making standards work®

Benefits of O-TTPF to Providers and Consumers

- *The ability to **work collaboratively** with peer organizations, suppliers and customers to define, review and approve the best approaches* developing a more trustworthy global technology supply chain
- *Industry members of the TTF can directly interact with government acquisition leaders through their participation in the forum and government members can interact with their suppliers in an open, neutral forum*
- *Market differentiation through the **future accreditation program**, and status as an organization that contributes to the Forum*
- *Members can network with their peers in similar organizations around the globe and help harmonize global technology supply chain initiatives*
- *The TTF is intended to benefit technology buyers across all industries concerned with **secure development practices and supply chain management**, including government and defense, transportation, healthcare and financial services*

THE Open GROUP
Making standards work®

Envisioned O-TTPF Accreditation Program

Trusted Technology Provider Framework (O-TTPF)
(Technology Supply Chain Best Practices)

O-TTFP Conformance and Evidence Criteria
(What a provider must do to adopt the O-TTPF)

O-TTPF Accreditation Policy
(How to assess a provider against the framework)

O-TTPF Accreditation Standard*

**Specification Authority = TTF*

O-TTPF Accreditation Assessment

Conducted by a 3rd Party Assessment Organization

Role: Evaluates the provider against the TTPF Accreditation Standard

Authorized Accreditation Organization(s)

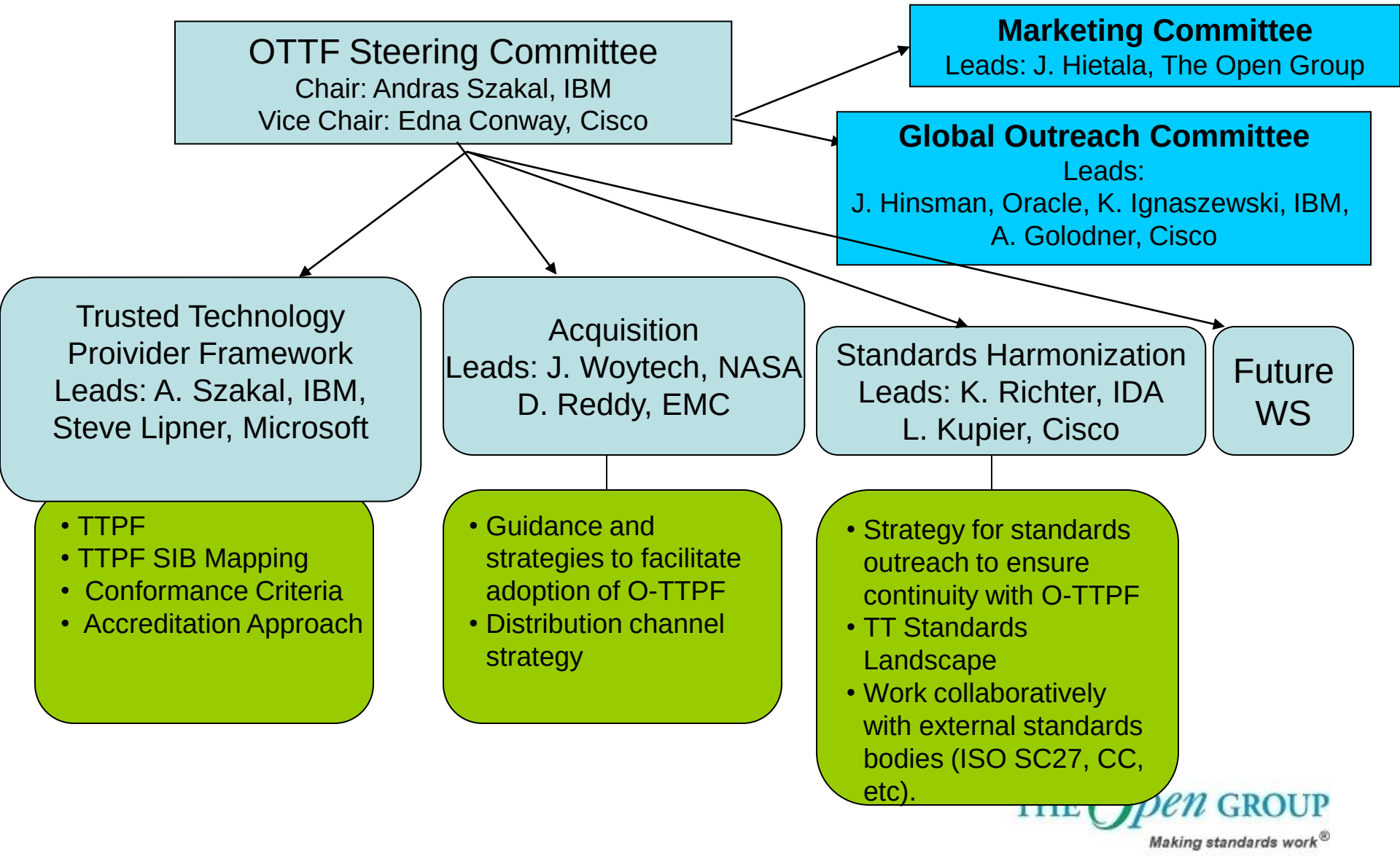
Accreditation Program Oversight

Conducted by the Accreditation Authority

Role: Manages Accreditation Registry, PR resolution, Accreditation Oversight

THE Open GROUP
Making standards work®

OTTF Governing Structure
(Current Work Streams and Committees)



THE Open GROUP
Making standards work®

Open Trusted Technology Provider Framework Work Stream

- The Trusted Technology Provider Framework (O-TTPF) will provide a framework for identifying
  - Technology supply chain best practices
  - Mapping to relevant standards and practices
  - Identify risks addressed by these practices
- The framework is intended to benefit technology buyers across all industries concerned with secure development practices and supply chain management.
- The framework is outcome based and not prescriptive
- The framework will identify the criteria and evidence necessary to determine if a provider has adopted specific practice
- The framework will define an accreditation program for assessing providers

Standards Harmonization Work Stream

- The Open Group and it's membership has extensive experience and a long track record in facilitating consensus across standards bodies to develop standards, including defining new standards, evolving existing ones, building consensus and providing support services, and developing best practices.

- A primary goal of the OTTF will be to facilitate consensus and rationalize efforts across global supply chain security standards efforts.

- The OTTF will provide a venue for establishing a unified voice for IT Vendors to provide input into international standards and policy initiatives related to supply chain integrity and secure engineering practices.

- This work stream will be focused on establishing relationships with existing standards groups and working to harmonize the O-TTPF across and between industry and global standards efforts

Trusted Technology Acquisition Work Stream

- The Acquisition work stream will produce guidance and strategies to support the acquisition process.

- The members of the acquisition work stream will feed valuable insight into their processes to ensure the O-TTPF is meaningfully adopted.

- The group will liaise with the members of other supply chain and logistics organizations to ensure that the O-TTPF is understood and integrated with existing supply chain management approaches.

THE Open GROUP
Making standards work®

Open Trusted Technology Forum Launch – December, 15th 2010

Thank You!

If you would like to participate in evolving this set of best practices and in helping to shape how this set of best practices will be used to indicate trustworthy products, and allow suppliers to " Build with Integrity" and governments and commercial entities as well to "Buy with Confidence", please contact Mike Hickey at: m.hickey@opengroup.org.

THE Open GROUP
Making standards work®

Example O-TTPF Conformance Requirements

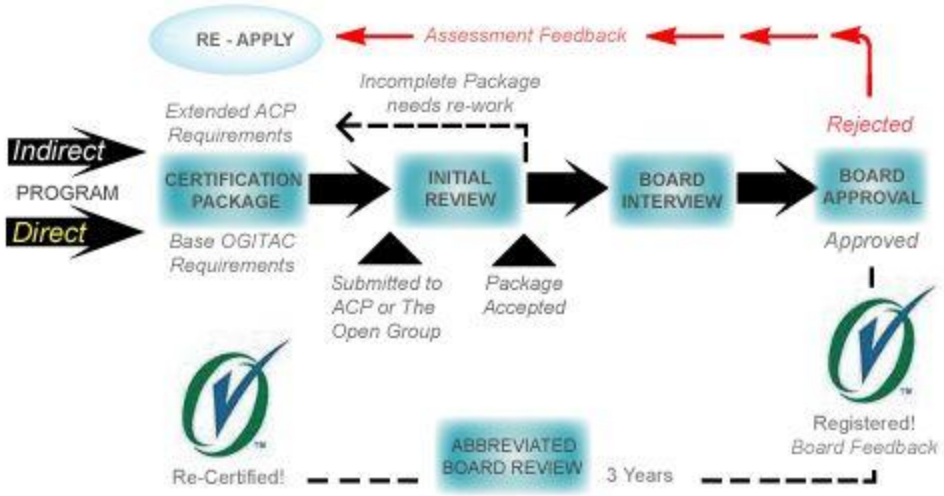
Industry Best Practice	Notes
Trusted technology providers utilize and internalize the application of a well-formed and documented development or manufacturing method or process.	Engineering/development methods are practical and meaningful within the vendor's domain of software, firmware, or hardware manufacturing as defined by the TTPF Method Guidance.

Best Practice Attribute	Attribute Definition
Requirements Management	Requirements are documented and traced back to product functionality.

Example Conformance Criteria

The Technology Provider documents product functional and non-functional requirements. Requirements can be traced back to implemented function. Evidence can be provided in the form of an electronic repository or paper document that describes where a requirement is realized in product function.

Example of a Successful Industry Certification Program



http://www.opengroup.org/itac/cert/

Certification Documents

» Certification Guide
» Certification Policy [PDF]
» Certification Agreement
» Certification TMLA
» Certification Package Templates
» Sample Certification Packages
» Recognized Methods
» Fee Schedule

Accreditation Documents

» Accreditation Guide
» Accreditation Policy [PDF]

» Accreditation Requirements [PDF]
» Accreditation Agreement [PDF]
» Accreditation TMLA [PDF]

» Conformance Statement Questionnaire
» Checklist

The Program is based upon four key documents:

- The **Certification Policy**, which sets out the policies and processes by which an IT Architect may achieve certification.
- The **Conformance Requirements**, in which the skills and experience that a Certified Architect must possess are documented
- The **Accreditation Policy**, which sets out the policies and processes by which an organization may achieve accreditation for its own certification program
- The **Accreditation Requirements**, in which the criteria that must be met by an Accredited Certification Program (ACP) are documented

THE Open GROUP
Making standards work®

Conformance documents

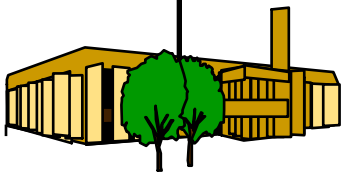
Conformance Requirements

Conformance Requirements
What a conforming organization must do to be accredited (documented in TTPF)

Conformance Statements
Public statement
How product meets conformance requirements

Customers

Check vendor claims



Vendors

Select appropriate tests

© 2004 The Open Group

THE Open GROUP
Making standards work®

Accreditation Program Phases

Accreditation Definition

- What can be certified or accredited
- Processes, policies, and procedures for certification
- How conformance will be demonstrated and validated

Implementation of Accreditation Program

Documents and software systems required to run the accreditation assessment program

Accreditation Program Operation

Ongoing process of accrediting the organization against the standards conformance criteria

© 2004 The Open Group

THE Open GROUP
Making standards work®

Recent TTF Blogs

IBM Institute for Advanced Security

Enabling innovation and collaboration on security issues facing our Smarter Planet

Home | About this blog

Search: type, hit

The IBM Institute for Advanced Security Expert Blog

Security and Supply Chains

Posted by Harriet Pearson on December 15, 2010 | Go to comments | Leave a comment (0)

Increasingly, the critical systems of the planet — telecommunications, banking, energy and others — depend on and benefit from the intelligence and interconnectedness enabled by existing and emerging technologies.

Whether these systems are trusted by the societies they serve depends in part on whether the technologies incorporated into them are fit for the purpose they are intended to serve. Of course, the leaders or owners of these systems have to do their part to achieve security and safety: e.g., to install, use and maintain technology appropriately, and to pay attention to people and process aspects such as insider threats. Cybersecurity considerations must be addressed in a sustainable way from the get-go, by design, and

RSS

Recent Posts

- Security and Supply
- Why I do security a
- Why I do cybersecu
- National Cybersecur

Search by Tag

cybersecurity secur

Sign me up!

Recent Tweets by The Open Group

- The Open Group welcomes Silver Member atsec information security corporation of the U.S. to the Trusted Technology Forum: http://ow.ly/3sLoE ~ 1 hour ago
- RT @togaftm: Share your TOGAF ideas, experiences, challenges and solutions at the free TOGAF Camp San Diego, Feb 9 http://ow.ly

'errated

IT: The professionals →

· 6:00 AM

↓ Jump to Comments

ed Technology Forum: Best practices for securing the global technology supply chain

By Mary Ann Davidson

Hello, I am Mary Ann Davidson. I am the Chief Security Officer for Oracle and I want to talk about The Open Group Trusted Technology Provider Framework (TTPF). What, you may ask, is that? The Trusted Technology Forum is an effort within The Open Group to develop a body of practices related to software and hardware manufacturing — the TTPF — that will address procurers' supply chain